Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión [*DOUE* L 194, de 19-VII-2016]

Seguridad de las redes y sistemas de información en la Unión Europea

Conocida como Directiva NIS (Network and Information Security), más comúnmente Directiva sobre ciberseguridad, viene a establecer medidas con el objeto de lograr un elevado nivel común de seguridad de las redes y sistemas de información dentro de la Unión a fin de mejorar el funcionamiento del mercado interior.

Su objetivo no es otro que, según su considerando sexto, formalizar «un planteamiento global en la Unión que integre requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, intercambio de información, cooperación y requisitos comunes de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales». Hay que partir de la premisa que considera que las redes y sistemas de información tienen atribuido un papel crucial en la sociedad, lo que provoca que su fiabilidad y seguridad sean esenciales para las actividades económicas y sociales, y en particular para el funcionamiento del mercado interior, lo que lleva a la UE a dictar la presente norma, ante la magnitud, frecuencia y efectos de los incidentes de seguridad que, de sobra es conocido, se están incrementando y representan una grave amenaza para el funcionamiento de las redes y sistemas de información.

Los sistemas y redes de información se han terminado por convertir en objetivo de acciones nocivas deliberadas destinadas a perjudicar o interrumpir su funcionamiento, interrumpiendo actividades económicas, lo que genera no sólo graves pérdidas financieras, sino que menoscaba la confianza del usuario y causa grandes daños a la economía de la Unión.

Las ventajas de las redes y sistemas de información, principalmente Internet, que contribuyen de forma decisiva a facilitar la circulación transfronteriza de productos, servicios y personas, son innegables. Pero es precisamente ese carácter transnacional el que produce que una perturbación grave de esas redes y sistemas, ya sea o no deliberada, y con independencia del lugar en que se produzca, puede afectar a diferentes Estados miembros y a la Unión en su conjunto. Por consiguiente, la seguridad de las redes y sistemas de información es fundamental para el correcto funcionamiento del mercado interior.

La presente Directiva busca que todos los Estados miembros posean unas capacidades mínimas y una estrategia que garanticen un elevado nivel de seguridad de las

Ars Iuris Salmanticensis,
vol. 5, junio 2017, 245-249
eISSN: 2340-5155

redes y sistemas de información en su territorio. Por otra parte, un segundo objetivo radica en que los operadores de servicios esenciales y los proveedores de servicios digitales estén sujetos a requisitos en materia de seguridad y notificación de incidentes, con el fin de fomentar una cultura de gestión de riesgos y garantizar que se informe de los incidentes más graves. Se entiende que las capacidades existentes no bastan para garantizar un elevado nivel de seguridad de las redes y sistemas de información que la Unión requiere. Por otra parte, los niveles de preparación de los Estados miembros son muy distintos, lo que ha dado lugar a planteamientos fragmentados en la Unión. Esta situación genera niveles desiguales de protección de los consumidores y las empresas, comprometiendo el nivel general de seguridad de las redes y sistemas de información de la Unión. A su vez, la inexistencia de requisitos comunes aplicables a los operadores de servicios esenciales y los proveedores de servicios digitales imposibilita la creación de un mecanismo global y eficaz de cooperación en la Unión. Las universidades y los centros de investigación tienen un papel determinante que desempeñar a la hora de impulsar la investigación, el desarrollo y la innovación en esos ámbitos. Para dar una respuesta efectiva a los problemas de seguridad de las redes y sistemas de información es necesario un planteamiento global en la Unión que integre requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, intercambio de información, cooperación y requisitos comunes de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales. No obstante, no está excluido que los operadores de servicios esenciales y los proveedores de servicios digitales apliquen medidas de seguridad más estrictas que las previstas en la presente Directiva.

A todo lo anterior hay que sumar que ciertos sectores de la economía ya están regulados o pueden regularse en el futuro con normas sectoriales que siempre que incluyan normas relacionadas con la seguridad de las redes y sistemas de información, por las que se impongan requisitos, de igual o mayor nivel, en materia de seguridad de las redes y sistemas de información o en materia de notificación de incidentes, se aplicarán en lugar de las disposiciones correspondientes de la presente Directiva.

Ante el panorama descrito, la Directiva sobre ciberseguridad deberá aplicarse tanto a los operadores de servicios esenciales como a los proveedores de servicios digitales, pero no a las empresas que suministren redes públicas de comunicaciones o presten servicios de comunicaciones electrónicas disponibles para el público, ni a los prestadores de servicios de confianza definidos en el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, que están sujetos a los requisitos de seguridad establecidos en dicho Reglamento.

Igualmente, esta Directiva deja en manos de los Estados miembros la adopción de las medidas necesarias para garantizar la protección de los intereses esenciales de su

Ars Iuris Salmanticensis,
vol. 5, junio 2017, 245-249
eISSN: 2340-5155

seguridad; preservar el orden público y la seguridad pública, y permitir la investigación, detección y enjuiciamiento de infracciones penales.

Sentadas estas bases, la Directiva aborda la regulación y la supervisión, a través de la imposición de medidas a adoptar por los principales sectores implicados. El sector bancario y de las infraestructuras de los mercados financieros es fundamental. El riesgo operativo es un componente fundamental de la regulación y la supervisión prudenciales en los sectores de la banca y las infraestructuras del mercado financiero. Dicho riesgo se extiende a todas las operaciones, incluidas la seguridad, la integridad y la resistencia de las redes y sistemas de información.

Los mercados en línea permiten a consumidores y comerciantes celebrar contratos de compraventa o de prestación de servicios en línea con comerciantes, y son el destino final de celebración de tales contratos. Esos mercados no deben tener por objeto servicios en línea que constituyan únicamente un paso intermedio para acceder a servicios prestados por terceros a través de los que finalmente se pueda celebrar un contrato. Por consiguiente, no deben tener por objeto servicios en línea que comparen el precio de los productos o servicios de diferentes comerciantes para luego dirigir al usuario hacia el comerciante al que este prefiera comprar el producto. Los servicios informáticos prestados por el mercado en línea pueden incluir servicios de tramitación de transacciones, agregación de datos o elaboración de perfiles de los usuarios.

En relación con el transporte marítimo y fluvial, los requisitos de seguridad que imponen los actos jurídicos de la Unión a las compañías, buques, instalaciones portuarias, puertos y servicios de gestión del tráfico de buques se aplican a la totalidad de las operaciones, incluidas las de los sistemas de radio y telecomunicaciones, los sistemas informáticos y las redes.

Para lograr un elevado nivel común de seguridad de las redes y sistemas de información dentro de la Unión a fin de mejorar el funcionamiento del mercado interior, la Directiva regula no sólo el objeto y ámbito de aplicación que acabamos de ver, también hace lo propio con el tratamiento de datos personales, la armonización mínima, las definiciones, la identificación de operadores de servicios esenciales y el concepto de efecto perturbador significativo.

A tal fin, la Directiva: a) establece obligaciones para todos los Estados miembros de adoptar una estrategia nacional de seguridad de las redes y sistemas de información; b) crea un Grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar la confianza y seguridad entre ellos; c) crea una red de equipos de respuesta a incidentes de seguridad informática (en lo sucesivo, «red de CSIRT», por sus siglas en inglés de «computer security incident response teams») con el fin de contribuir al desarrollo de la confianza y seguridad entre los Estados miembros y promover una cooperación operativa rápida y eficaz; y d) establece requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales.

Ars Iuris Salmanticensis,
vol. 5, junio 2017, 245-249
eISSN: 2340-5155

Entre las definiciones, recoge las de «redes y sistemas de información»; «seguridad de las redes y sistemas de información»; «estrategia nacional de seguridad de las redes y sistemas de información»; «operador de servicios esenciales»; «servicio digital»; «proveedor de servicios digitales»; «incidente»; «gestión de incidentes»; «riesgo»; «representante»; «norma»; «especificación»; «punto de intercambio de internet (IXP)»; «servidor de sistema de nombres de dominio (DNS)»; «proveedor de servicios de DNS»; «registro de nombres de dominio de primer nivel»; «mercado en línea»; «motor de búsqueda en línea», y «servicio de computación en nube».

Por otra parte, también se define la Estrategia nacional de seguridad de las redes y sistemas de información; las Autoridades nacionales competentes y punto de contacto único; los Equipos de respuesta a incidentes de seguridad informática (CSIRT) y la Cooperación a escala nacional. En este sentido, se atribuye a cada Estado miembro la potestad para adoptar una estrategia nacional de seguridad de las redes y sistemas de información que establezca los objetivos estratégicos y las medidas políticas y normativas adecuadas con objeto de alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información y que cubra al menos los sectores que figuran en el anexo II y los servicios que figuran en el anexo III de la propia Directiva.

A fin de apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar confianza y seguridad, y buscando procurar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, se establece un Grupo de cooperación que ejercerá sus funciones con arreglo a una serie de programas de trabajo bienales.

En materia de seguridad y notificación de incidentes y la Aplicación y observancia, dispone la Directiva que serán también los Estados miembros quienes velarán por que los operadores de servicios esenciales tomen las medidas técnicas y de organización adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información que utilizan en sus operaciones. Habida cuenta de la situación, dichas medidas garantizarán un nivel de seguridad de las redes y sistemas de información adecuado en relación con el riesgo planteado.

Finalmente, la presente Directiva regula los Requisitos en materia de seguridad y notificación de incidentes; la Aplicación y observancia y la Jurisdicción y territorialidad. Y lo hace nuevamente recurriendo a la técnica por la que serán los Estados miembros quienes garanticen que los proveedores de servicios digitales determinen y adopten medidas técnicas y organizativas adecuadas y proporcionadas para gestionar los riesgos, teniendo en cuenta los avances técnicos, dichas medidas garantizarán un nivel de seguridad de las redes y los sistemas de información adecuado en relación con el riesgo planteado existente para la seguridad de las redes y sistemas de información que se utilizan en el marco de la oferta de servicios en la Unión.

De igual modo, los Estados miembros fomentarán, sin imponer ni favorecer el uso de un tipo específico de tecnología, la utilización de normas y especificaciones

Ars Iuris Salmanticensis,
vol. 5, junio 2017, 245-249
eISSN: 2340-5155

aceptadas a nivel europeo o internacionalmente que sean pertinentes en materia de seguridad de las redes y sistemas de información.

En definitiva, se trata de una norma que obliga a diferentes sujetos a adoptar medidas cuyo fin último es la garantía de un elevado nivel común de seguridad de las redes y sistemas de información, al tiempo que crea varios grupos y redes que serán fundamentales en el intercambio de información clave y en la respuesta, en su caso, ante incidentes de seguridad.

Daniel TERRÓN SANTOS
Profesor Ayudante Doctor de Derecho Administrativo
Universidad de Salamanca
datersa@usal.es

Ars Iuris Salmanticensis,
vol. 5, junio 2017, 245-249
eISSN: 2340-5155